JAMMING REPORT

ABSTRACT

Jamming attacks pose a significant threat to cyber-physical systems (CPS), such as drones, by disrupting their communication channels. In this experiment, we implemented and analyzed four different types of jamming attacks: Continuous Wave (CW) Jamming, Sweeping Jamming, Pulsed Noise Jamming, and Directional Jamming. The objective was to understand how these attacks impact drone navigation and communication within the ADS-B (Mode S Extended Squitter transponder - 1090ES) channel.

Keywords—jamming, cybersecurity, CPS, drone communication, ADS-B

INTRODUCTION

Jamming attacks are a critical cybersecurity threat to **Cyber-Physical Systems (CPS)**, particularly **Unmanned Aerial Vehicles (UAVs)**, disrupting their communication and navigation. Drones rely on **Automatic Dependent Surveillance–Broadcast (ADS-B)** to transmit real-time positional data to ground control stations (GCS). However, jamming interferes with these signals, causing drones to lose connectivity or deviate from their intended path. This study explores **four types of jamming attacks**—Continuous Wave (CW), Sweeping, Pulsed Noise, and Directional Jamming—by implementing them in a simulated drone environment. By evaluating their impact, we aim to understand how **different jamming techniques affect UAV operations** and propose mitigation strategies. Addressing these vulnerabilities is crucial for ensuring **secure and resilient drone networks** in both civilian and military applications.

TYPES OF JAMMING ATTACKS

A. Continuous Wave (CW) Jamming

- Introduces a constant noise signal that gradually increases over time.
- Causes drones to lose communication as the jamming effect strengthens.

B. Sweeping Jamming

- Mimics a frequency-hopping jammer with periodic fluctuations.
- Results in intermittent loss of communication, making drone tracking unstable.

C. Pulsed Noise Jamming

- Introduces intermittent bursts of interference.
-
- Leads to sporadic message loss affecting real-time drone navigation.

D. Directional Jamming

- Targets drones within a predefined geographic area.
- Causes localized interference without affecting drones outside the range.

IMPLEMENTATION

The jamming mechanisms were integrated into the **Drone-Sim** project by modifying the Jammer class and simulation scripts:

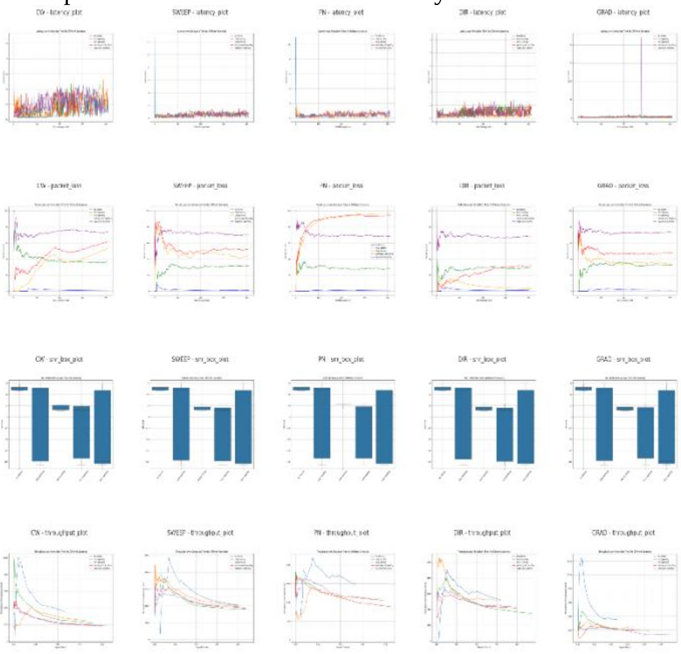
1. ***jammer.py:*** Defines jamming probability, noise intensity, and signal degradation.
2. ***cw_jamming_s.py:*** Implements gradual increase in jamming power.
3. ***sweeping_jamming_s.py***: Introduces periodic variations in interference intensity.
4. ***pulsated_noise_jamming_s.py*****:** Generates intermittent signal loss.
5. ***directional_jamming_s.py*****:** Targets drones in a specific geographic area.

JAMMING TYPE	EFFECT	IMPLEMENTATION
Continuous Wave (CW) Jamming	Gradually increases over time	frame / 100 increases jamming strength
Sweeping Jamming	Periodic signal interference	Sinusoidal wave (sin(frame / 5)) affects probability
Pulsed Noise Jamming	Short bursts of jamming	Sinusoidal wave (sin(frame / 10)) creates intermittent jamming
Directional Jamming	Jamming only in a specific area	Geographic check (distance <= radius) applies interference

Table 1 : Comparison of Jamming Techniques and Their UAV Impact

RESULTS AND OBSERVATIONS

1. ***Latency Plot (latency_plot.png)****:* Shows how different jamming techniques affect drone communication delays.
2. ***Packet Loss (packet_loss.png)****:* Illustrates how much data transmission is lost under each jamming attack.
3. ***SNR Box Plot (snr_box_plot.png)****:* Represents the signal-to-noise ratio variations caused by jamming.
4. ***Throughput Plot (throughput_plot.png)****:* Displays the impact on data transmission efficiency.



Latency Analysis*:*

- **CW Jamming** shows a gradual increase in latency, indicating progressive interference.
- **Sweeping Jamming** causes fluctuations in latency, reflecting periodic signal disruptions.
- **Pulsed Noise Jamming** results in intermittent latency spikes, disrupting real-time control.
- **Directional Jamming** has localized effects, impacting latency only within the jamming zone.
- **Gradual Jamming** shows a continuous but controlled rise in latency.

Packet Loss*:*

- **CW Jamming** results in increasing packet loss as jamming power intensifies.
- **Sweeping Jamming** exhibits intermittent packet **drops**, affecting communication stability.
- **Pulsed Noise Jamming** leads to sporadic packet loss, causing navigation uncertainty.
- **Directional Jamming** shows high packet loss within affected areas, but no impact elsewhere.
- **Gradual Jamming** gradually increases packet loss over time.

SNR (Signal-to-Noise Ratio)*:*

- **CW Jamming** shows a continuous drop in SNR, indicating sustained interference.
- **Sweeping Jamming** results in SNR variations, reflecting periodic disturbances.
- **Pulsed Noise Jamming** has fluctuating SNR, with brief signal recoveries.
- **Directional Jamming** only degrades SNR in specific regions.
- **Gradual Jamming** slowly reduces SNR, correlating with increasing interference.

Throughput Impact*:*

- **CW Jamming** significantly reduces throughput over time, limiting data transmission.
- **Sweeping Jamming** causes throughput to fluctuate, reflecting periods of connectivity loss.
- **Pulsed Noise Jamming** results in momentary drops in throughput, affecting real-time control.
- **Directional Jamming** only affects throughput in targeted locations.
- **Gradual Jamming** shows a steady decline in throughput, mirroring increasing interference.

CONCLUSION

The study highlights that jamming attacks severely impact drone communication and navigation, with varying effects depending on the jamming method. Continuous Wave Jamming leads to gradual performance degradation, Sweeping Jamming creates intermittent interference, Pulsed Noise Jamming disrupts drone connectivity sporadically, and Directional Jamming selectively affects drones within a specific zone. These vulnerabilities emphasize the need for advanced countermeasures**,** such as frequency hopping, adaptive filtering, encryption, and multi-sensor fusion, to ensure UAV resilience in real-world applications. Future research should focus on real-time detection and mitigation strategies to enhance drone security and operational stability in adversarial environments.

REFERENCES

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201-220, 2005.

[2] M. Lichtman, R. Tandon, and T. Clancy, "Jamming Techniques and Countermeasures in Wireless Networks: A Survey," Proceedings of the IEEE, vol. 107, no. 4, pp. 570-594, 2019.

[3] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," IEEE Communications Magazine, vol. 54, no. 5, pp. 36-42, 2016.

[4] J. Wang, Y. Chen, and T. Jiang, "Jamming-Resistant UAV Communication Networks Based on Deep Reinforcement Learning," IEEE Transactions on Wireless Communications, vol. 20, no. 5, pp. 3455-3469, 2021.